**Friends of the Page-Walker Hotel**

**Information Security Policy**

# Introduction

This policy covers the security of organization information and must be distributed to all directors. The Board of Directors will review and update this information security policy at least once a year to incorporate relevant security needs that may develop. Each director must read and sign a form verifying they have read and understand this policy.

# Ethics and Acceptable Use Policies

The Friends of the Page-Walker Hotel expects that all directors conduct themselves in a professional and ethical manner. A director should not conduct business that is unethical or illegal in any way, nor should a director influence others to act unethically or illegally. Furthermore, a director should report any dishonest activities or damaging conduct to the board.

Security of organization information is extremely important to our mission. We are trusted by those we serve to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal information (e.g., name, address, phone number, email, Social Security number, driver’s license number, bank account, credit card numbers, etc.) or organization information not publicly available (e.g., financial information, director information, plans, etc.). It is important the directors do not reveal sensitive information about our organization to outside resources that do not need to know such information.

# Usage Policy

The Friends of the Page-Walker Hotel expects all directors to do their best to protect user information. Any device used to access personal information shall have active and updated antivirus and security programs. The Friends of the Page-Walker Hotel does not allow the storage of client personal information on home computers such as Social Security numbers or any bank account and financial information. The use of removable electronic media is also prohibited for storing credit card information.

Directors are prohibited from receiving and storing personal client information on their home computers. Directors are expected to protect organization passwords or other information used to access organization data. The proper use of email is also expected. Directors are prohibited from emailing or utilizing chat or messaging programs to transmit personally identifiable information that may lead to that information being compromised. For example, it is prohibited to email Social Security numbers or credit card numbers.

# Disciplinary Action

A director’s failure to comply with the standards and policies set forth in this document may result in disciplinary action up to and including removal from the board.

# Protect Stored Data

Protect sensitive information stored or handled by the organization. All sensitive information must be stored securely. Any media (e.g., paper, computer hard drive, flash drive, etc.) that contain sensitive information must be protected against unauthorized access. Media no longer needed must be destroyed in such a manner to render sensitive data irrecoverable (e.g., shredding, disassembly, etc.).

***Credit Card Information Handling Specifics***

* Destroy cardholder information in a secure method when no longer needed. Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable.
* It is prohibited to store the contents of the credit card magnetic strip (track data) on any media whatsoever.
* It is prohibited to store the card validation code (3 or 4 digit value printed on the signature panel of the card) or PIN number on any media whatsoever.
* All but the last 4 numbers of the credit card account number must be masked (e.g., x’s or \*’s) when the number is displayed electronically or on paper.

# Restrict Access to Data

Restrict access to sensitive information (organization data and personal information) to those that have a need-to-know. No directors should have access to credit card account numbers unless they have a specific job function that requires such access.

# Physical Security

Restrict physical access to sensitive information or systems that house that information (e.g., computers or filing cabinets storing cardholder data) to protect it from those who do not need to access that information. Media is defined as any printed or handwritten paper, received faxes, floppy disks, backup tapes, computer hard drive, etc. All cardholder data should be labeled as confidential and securely stored. If media needs to be shipped, it will be done by a secure courier or by using a shipping method that can be accurately tracked.

The Friends of the Page-Walker Hotel will keep on record all credit card forms in a secure file for six months to cover the chargeback window. After that all forms containing the full credit card number will be shredded and disposed of.

* Media containing sensitive information must be securely handled and distributed.
* Media containing sensitive information (especially credit card account numbers and Social Security numbers) should be properly inventoried and disposed of when no longer needed for business by deleting, shredding, incinerating, or degaussing before disposal so that it cannot be reconstructed.
* Any computers that may contain sensitive information must be password protected.

# Security Awareness and Procedures

Keeping sensitive information secure requires periodic training to keep security awareness levels high. The following organization policies and procedures address this issue.

* The board of directors will review and discuss this policy annually at a regular meeting of the board.
* Directors are required to read this security policy and verify that they understand it by signing an acknowledgement form (see Appendix A).
* All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI-DSS).
* All third parties with access to personal information will be reviewed and approved by the board of directors prior to engagement.

# Security Management/Incident Response Plan

The President of the Board of Directors is responsible for communicating security policies to the Board and tracking adherence to policies. In the event of a compromise of sensitive information, the President will oversee the execution of the incident response plan. In the instance of suspected fraud or a breach in the system, the President should be notified immediately.

***Incident Response Plan***

1. If a compromise is suspected, alert the President of the Board of Directors**.**
2. The President will conduct an initial investigation of the suspected compromise.
3. If compromise of information is confirmed, the President will the Board of Directors and begin informing parties that may be affected by the compromise. If the compromise involves credit card account numbers, perform the following:
* Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.
* Alert necessary parties (Merchant Bank, Visa Fraud Control, law enforcement).
* Provide compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours.
* More Information

<https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf>

# *Appendix A – List of Service Providers*

List of Service Providers – <https://www.visa.com/splisting/>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Provider** | **Type** | **Contact** | **Contact Number** | **PCI Compliance Requirement** |
| Affinipay | Payment Processor | Affinipay.com | 855.656.4685 | Affinipay and Friends of the Page-Walker Hotel |
| Wild Apricot | Website Host | Wildapricot.com | 877.493.6090 | Provider |
| Square | Payment Processor | Squareup.com | 855.700.6000 | Provider |
|  |  |  |  |  |

# *Appendix B- Director Agreement*

Agreement to Comply with Information Security Policy

Director Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I agree to take all reasonable precautions to assure that organization internal information, or information that has been entrusted to the organization by third parties such as members, will not be disclosed to unauthorized persons. At the end of my involvement with the organization, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the President.

I have access to a copy of the Information Security Policy, I have read and understand the policy, and I understand how it impacts me. As a condition of continued service, I agree to abide by the policy and other requirements found in the organization security policy. I understand that non-compliance will be cause for disciplinary action up to and including removal from the board and perhaps criminal and/or civil penalties.

I also agree to promptly report all violation or suspected violations of information security policies to the Board of Directors.

 X\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Director’s signature